Vorex and Authanvil - SAML 2.0 Single Sign-On (SSO) Just-in-Time (JIT) Provisioning

User Guide | September 2021

Vorex and Authanvil - SAML 2.0 Single Sign-On (SSO) Just-in-Time (JIT) Provisioning

Release 5.4.0 | Version 1.0

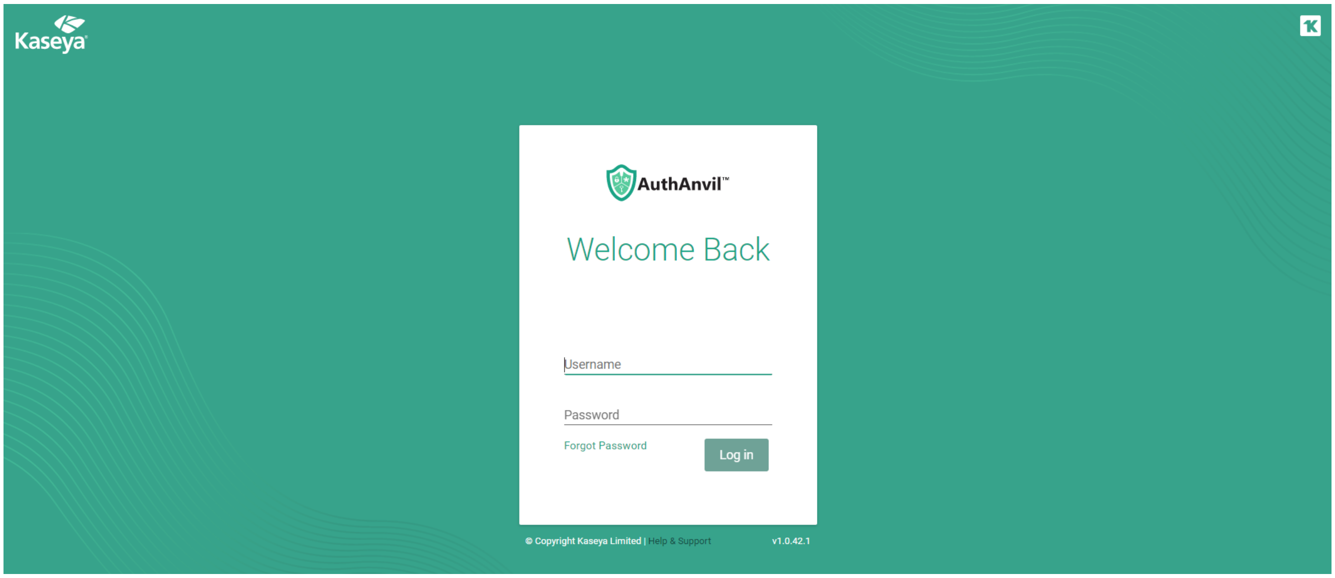
Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement.

Contents

AuthAnvil Setup

Assuming you have an active AuthAnvil (https://subdomain.authanvil.com/) account.



In order to setup Vorex with AuthAnvil you need to have a user group that can associate with the Vorex SSO configuration.

Creating a new group.

1 Log in to AuthAnvil and navigate to Directory Manager > Groups.

2 Click the + button to create a new group.

3 Give a name to your group.

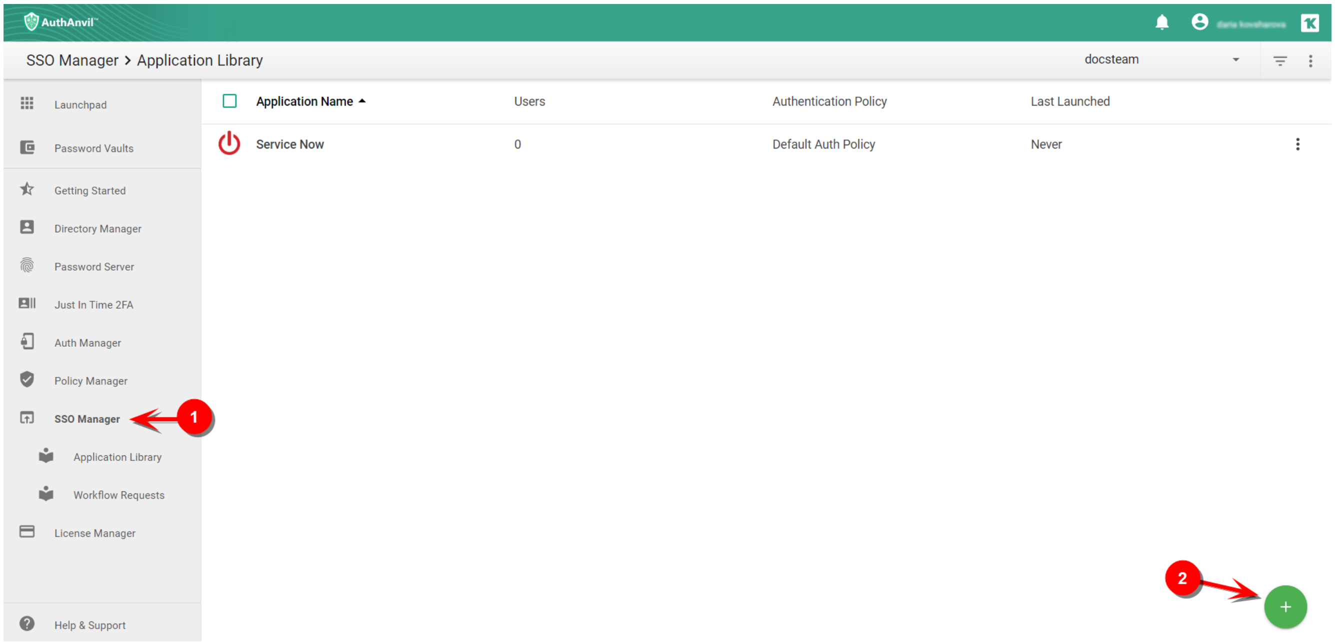
4 Click the **Add Group** button.

Now a new group is created.

Setting up Vorex with AuthAnvil.

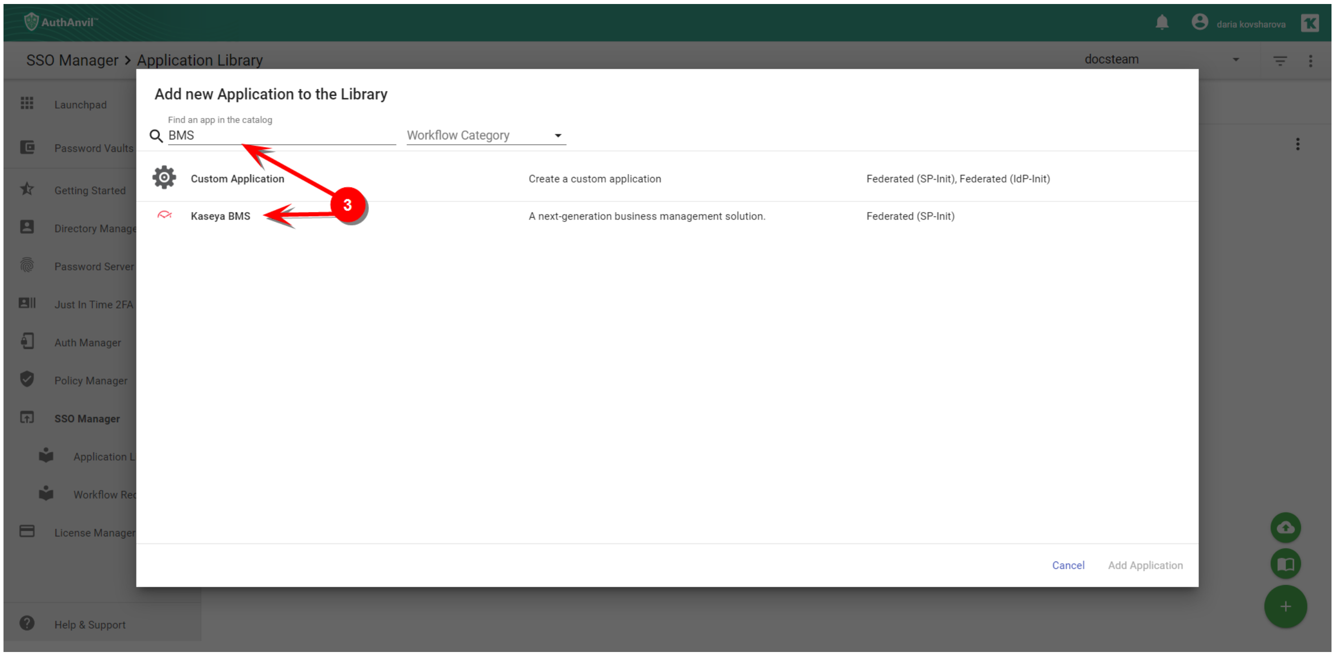
1 Navigate to SSO Manager.

2 Click the + button.



Application Name	Users	Authentication Policy	Last Launched
Service Now	0	Default Auth Policy	Never

3 Click the 📖 button then search for Vorex and then select Vorex from the list.



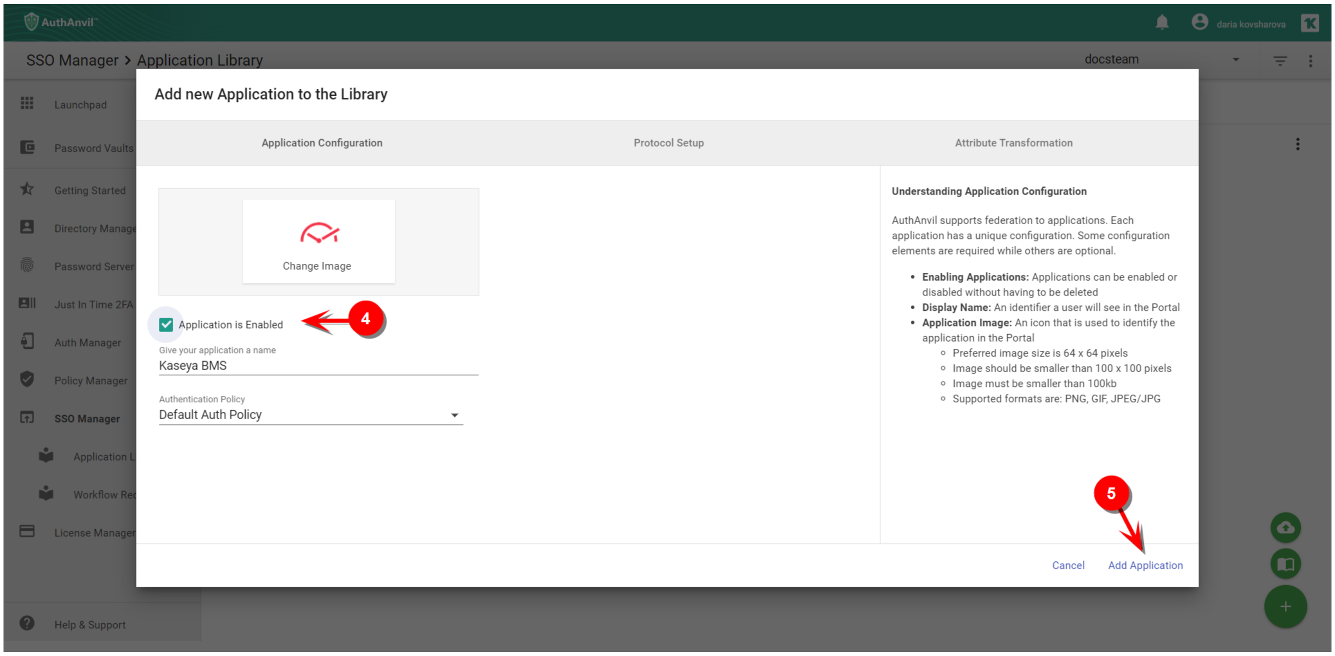
Add new Application to the Library

Find an app in the catalog: BMS

Custom Application	Create a custom application	Federated (SP-Init), Federated (IdP-Init)
Kaseya BMS	A next-generation business management solution.	Federated (SP-Init)

4 In the **Add new Application to the Library** window, select the Application is Enabled checkbox.

5 Click the **Add Application** button at the bottom right of the screen.



Add new Application to the Library

☑ Application is Enabled

Give your application a name
Kaseya BMS

Authentication Policy
Default Auth Policy

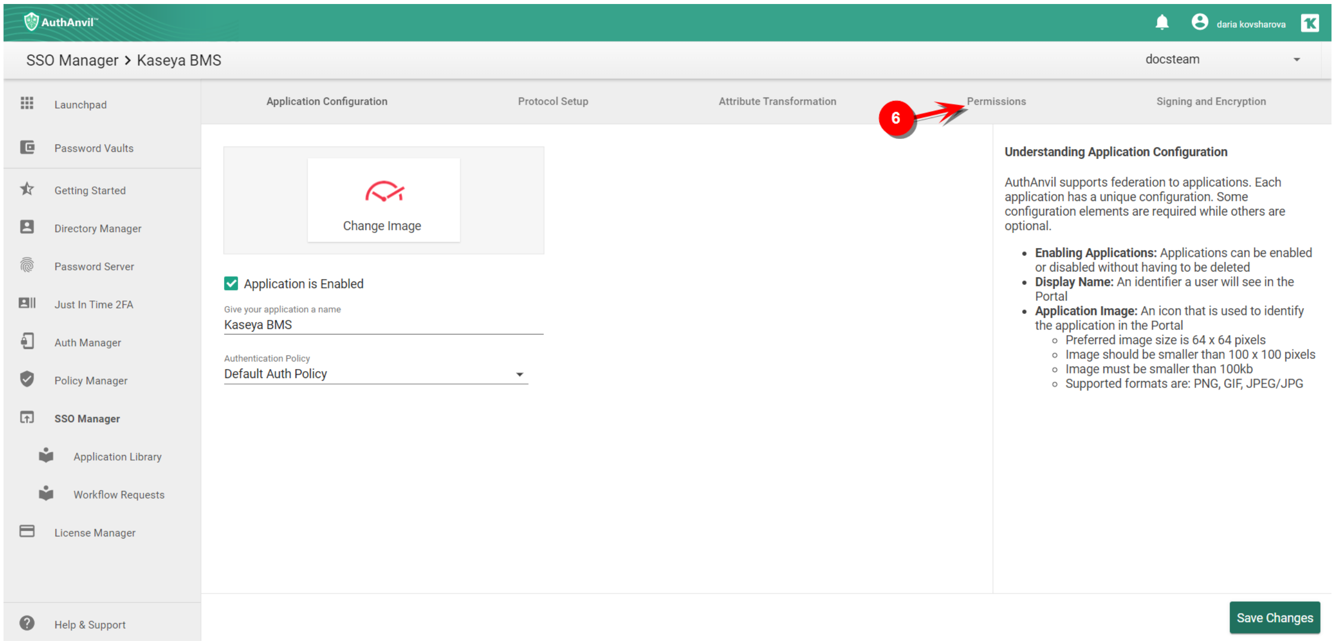
Understanding Application Configuration

AuthAnvil supports federation to applications. Each application has a unique configuration. Some configuration elements are required while others are optional.

- **Enabling Applications:** Applications can be enabled or disabled without having to be deleted
- **Display Name:** An identifier a user will see in the Portal
- **Application Image:** An icon that is used to identify the application in the Portal
  - Preferred image size is 64 x 64 pixels
  - Image should be smaller than 100 x 100 pixels
  - Image must be smaller than 100kb
  - Supported formats are: PNG, GIF, JPEG/JPG

Now the application added.

6 Navigate to **Permissions** tab.



☑ Application is Enabled

Give your application a name
Kaseya BMS

Authentication Policy
Default Auth Policy

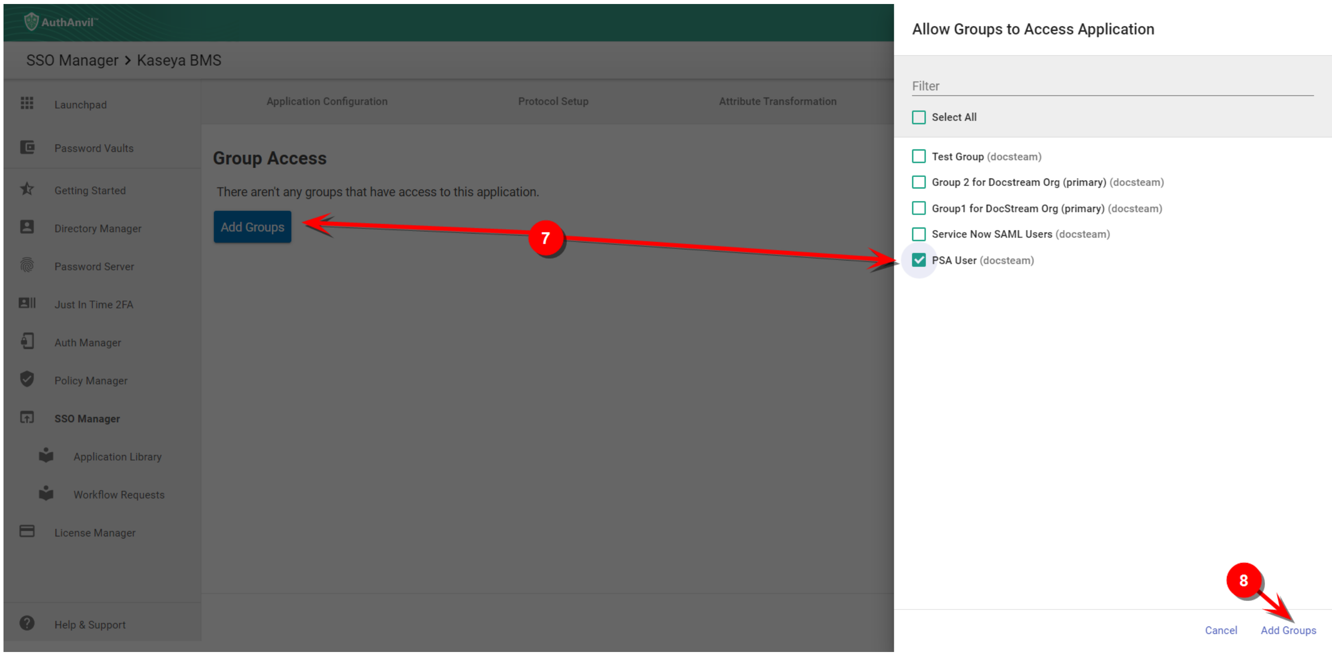
Understanding Application Configuration

AuthAnvil supports federation to applications. Each application has a unique configuration. Some configuration elements are required while others are optional.

- **Enabling Applications:** Applications can be enabled or disabled without having to be deleted
- **Display Name:** An identifier a user will see in the Portal
- **Application Image:** An icon that is used to identify the application in the Portal
  - Preferred image size is 64 x 64 pixels
  - Image should be smaller than 100 x 100 pixels
  - Image must be smaller than 100kb
  - Supported formats are: PNG, GIF, JPEG/JPG

7 Click the **Add Group** button and select the group you created.

8 Click the **Add Groups** button to finish setup.



Group Access

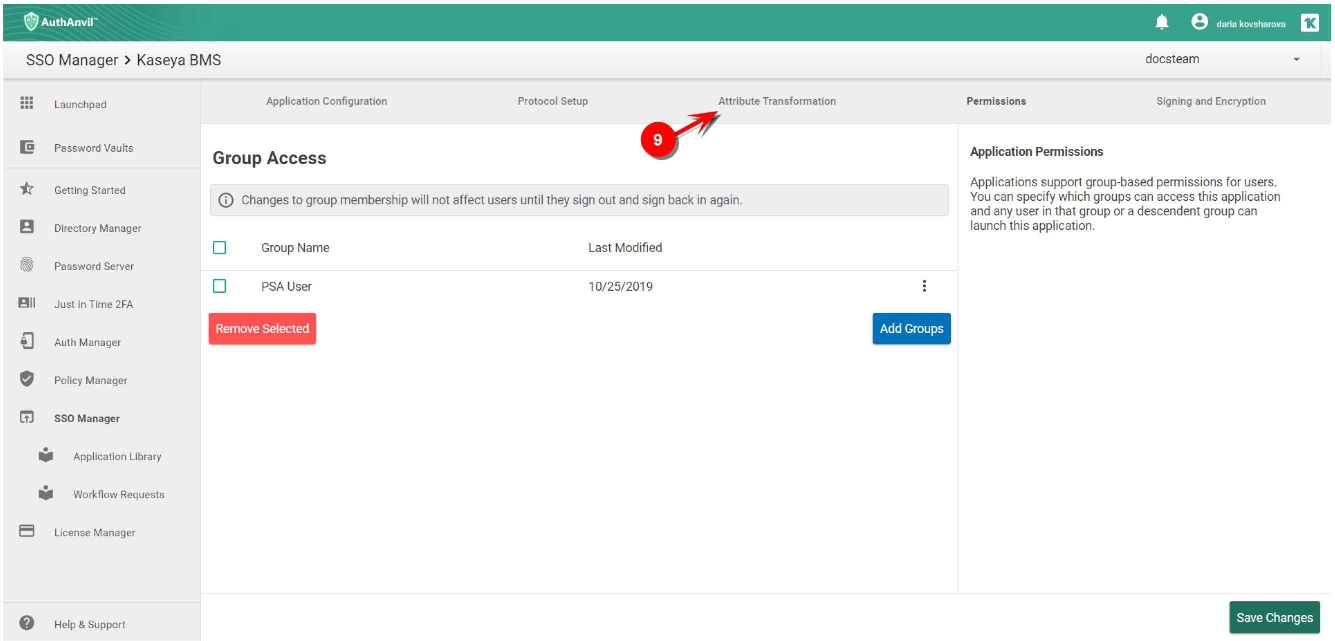
There aren't any groups that have access to this application.

Allow Groups to Access Application

□ Select All

□ Test Group (docsteam)
□ Group 2 for Docstream Org (primary) (docsteam)
□ Group1 for DocStream Org (primary) (docsteam)
□ Service Now SAML Users (docsteam)
☑ PSA User (docsteam)

9 Navigate to **Attribute Transformation** tab.



Group Access

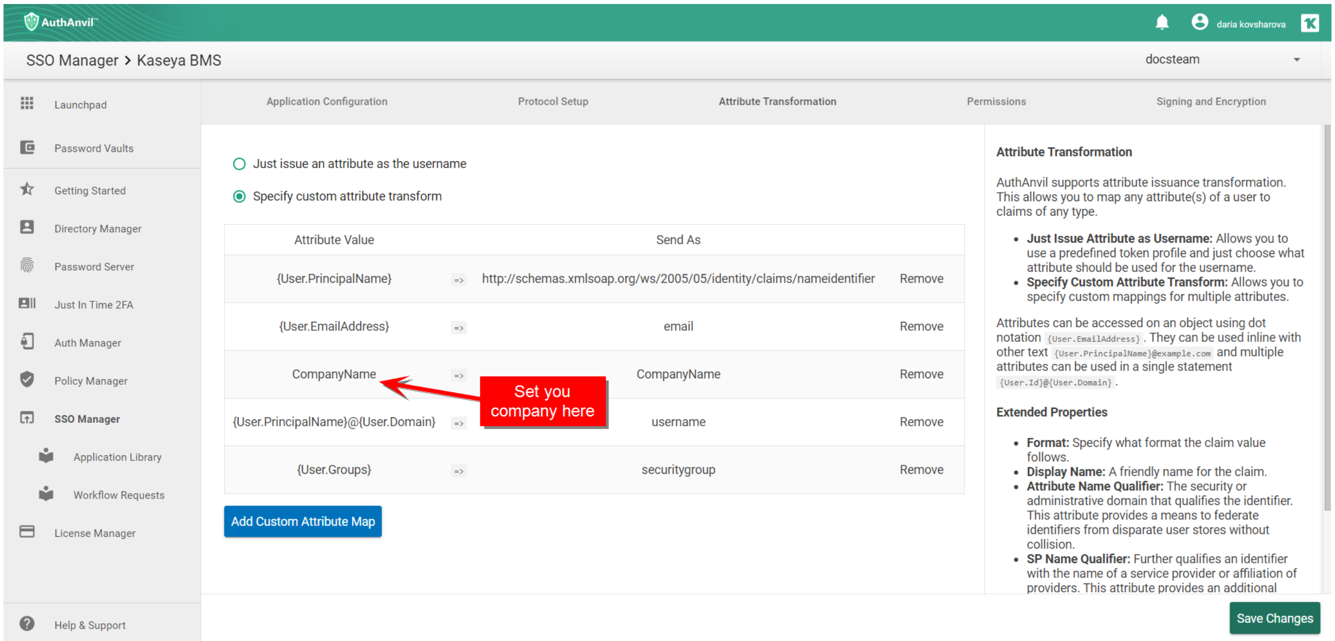
ⓘ Changes to group membership will not affect users until they sign out and sign back in again.

□	Group Name	Last Modified
□	PSA User	10/25/2019

Application Permissions

Applications support group-based permissions for users. You can specify which groups can access this application and any user in that group or a descendent group can launch this application.

10 Change the **CompanyName** attribute



○ Just issue an attribute as the username

● Specify custom attribute transform

Attribute Value		Send As	
{User.PrincipalName}	=>	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	Remove
{User.EmailAddress}	=>	email	Remove
CompanyName	=>	CompanyName	Remove
{User.PrincipalName}@{User.Domain}	=>	username	Remove
{User.Groups}	=>	securitygroup	Remove

Attribute Transformation

AuthAnvil supports attribute issuance transformation. This allows you to map any attribute(s) of a user to claims of any type.

- **Just Issue Attribute as Username:** Allows you to use a predefined token profile and just choose what attribute should be used for the username.
- **Specify Custom Attribute Transform:** Allows you to specify custom mappings for multiple attributes.

Attributes can be accessed on an object using dot notation `{User.EmailAddress}`. They can be used inline with other text `{User.PrincipalName}@example.com` and multiple attributes can be used in a single statement `{User.Id}@{User.Domain}`.

Extended Properties

- **Format:** Specify what format the claim value follows.
- **Display Name:** A friendly name for the claim.
- **Attribute Name Qualifier:** The security or administrative domain that qualifies the identifier. This attribute provides a means to federate identifiers from disparate user stores without collision.
- **SP Name Qualifier:** Further qualifies an identifier with the name of a service provider or affiliation of providers. This attribute provides an additional

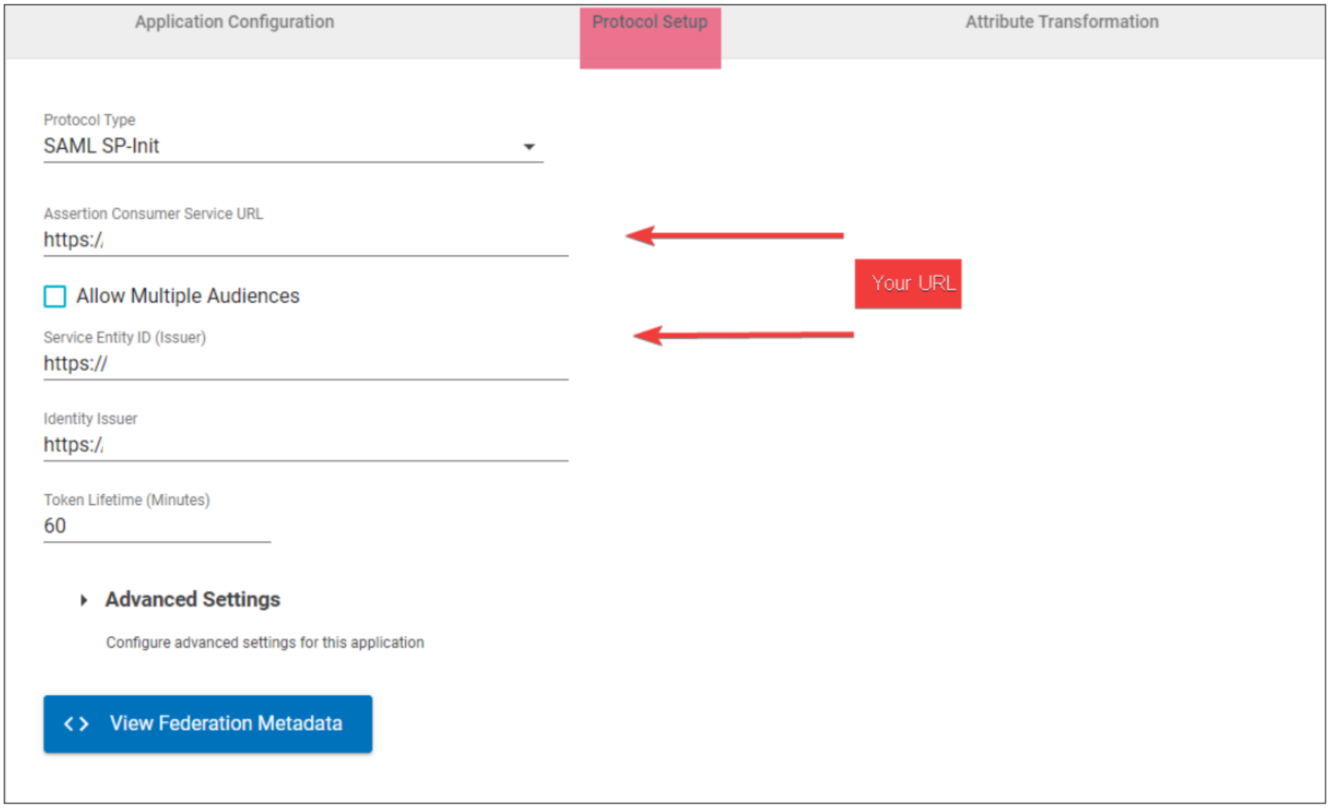
Protocol Setup

1 Navigate to the **Protocol Setup** tab.

2 For Assertion Consumer URL, change the base url to the base url of your BMS server. In the example below, the base url is `na1bmspreview.kaseya.com`.

3 For **Service Entity ID**, change the base url to the base url of your BMS server. In the example below, the base url is `na1bmspreview.kaseya.com`.

4 Save your changes.



Protocol Type
SAML SP-Init

Assertion Consumer Service URL
https:/,

□ Allow Multiple Audiences

Service Entity ID (Issuer)
https://

Identity Issuer
https:/,

Token Lifetime (Minutes)
60

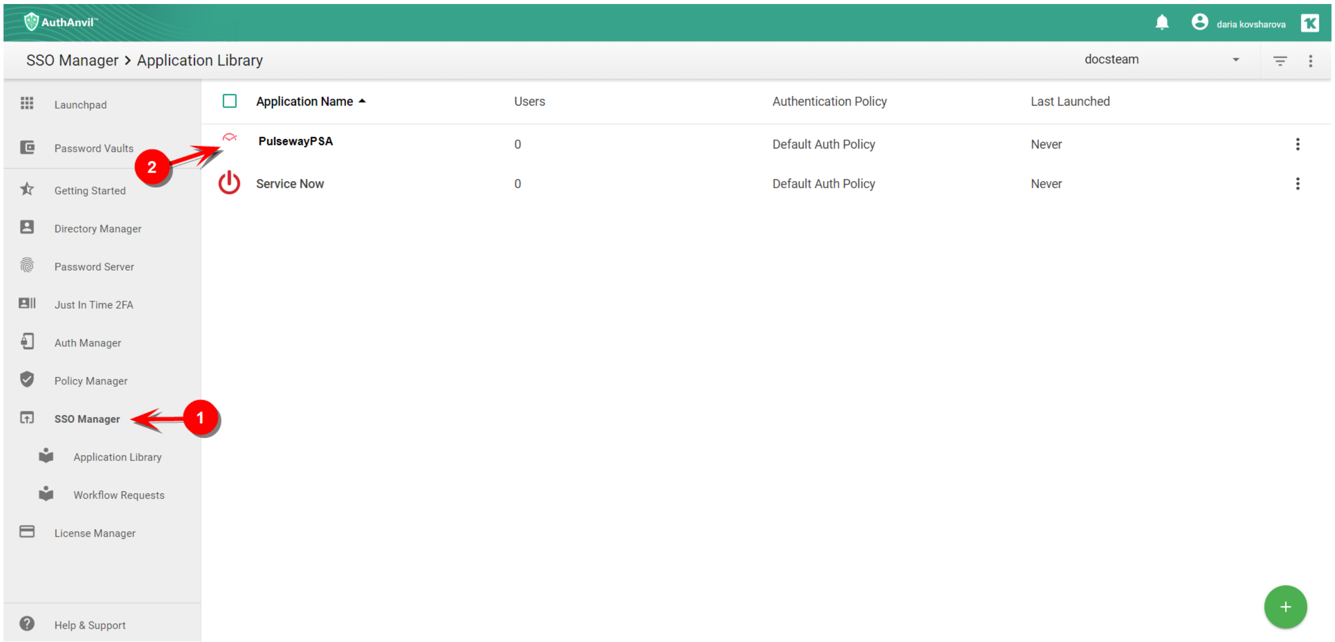
Advanced Settings

Configure advanced settings for this application

Download the Certificate

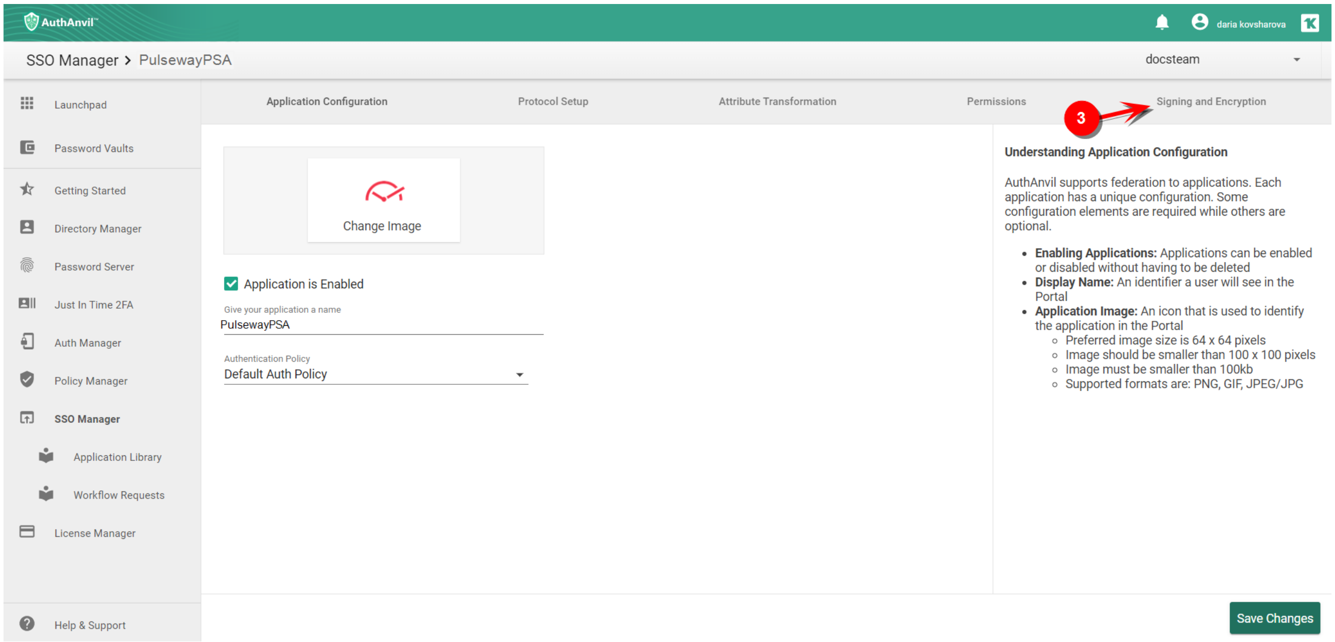
1 Navigate to AuthAnvil > SSO Manager.

2 Open the Vorex application.



Application Name	Users	Authentication Policy	Last Launched
PulsewayPSA	0	Default Auth Policy	Never
Service Now	0	Default Auth Policy	Never

3 Navigate to **Signing and Encryption** tab.



☑ Application is Enabled

Give your application a name
PulsewayPSA

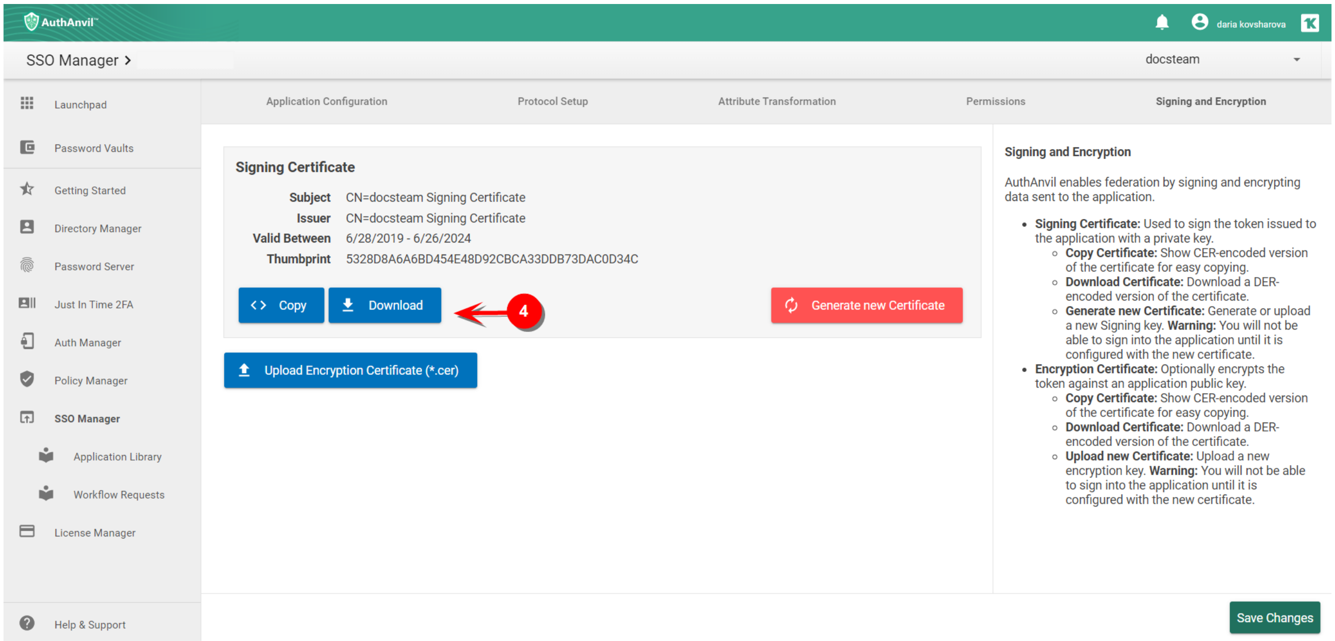
Authentication Policy
Default Auth Policy

Understanding Application Configuration

AuthAnvil supports federation to applications. Each application has a unique configuration. Some configuration elements are required while others are optional.

- **Enabling Applications:** Applications can be enabled or disabled without having to be deleted
- **Display Name:** An identifier a user will see in the Portal
- **Application Image:** An icon that is used to identify the application in the Portal
  - Preferred image size is 64 x 64 pixels
  - Image should be smaller than 100 x 100 pixels
  - Image must be smaller than 100kb
  - Supported formats are: PNG, GIF, JPEG/JPG

4 Click the **Download** button.



Signing Certificate

Subject CN=docsteam Signing Certificate
Issuer CN=docsteam Signing Certificate
Valid Between 6/28/2019 - 6/26/2024
Thumbprint 5328D8A6A6BD454E48D92CBCA33DDB73DAC0D34C

Signing and Encryption

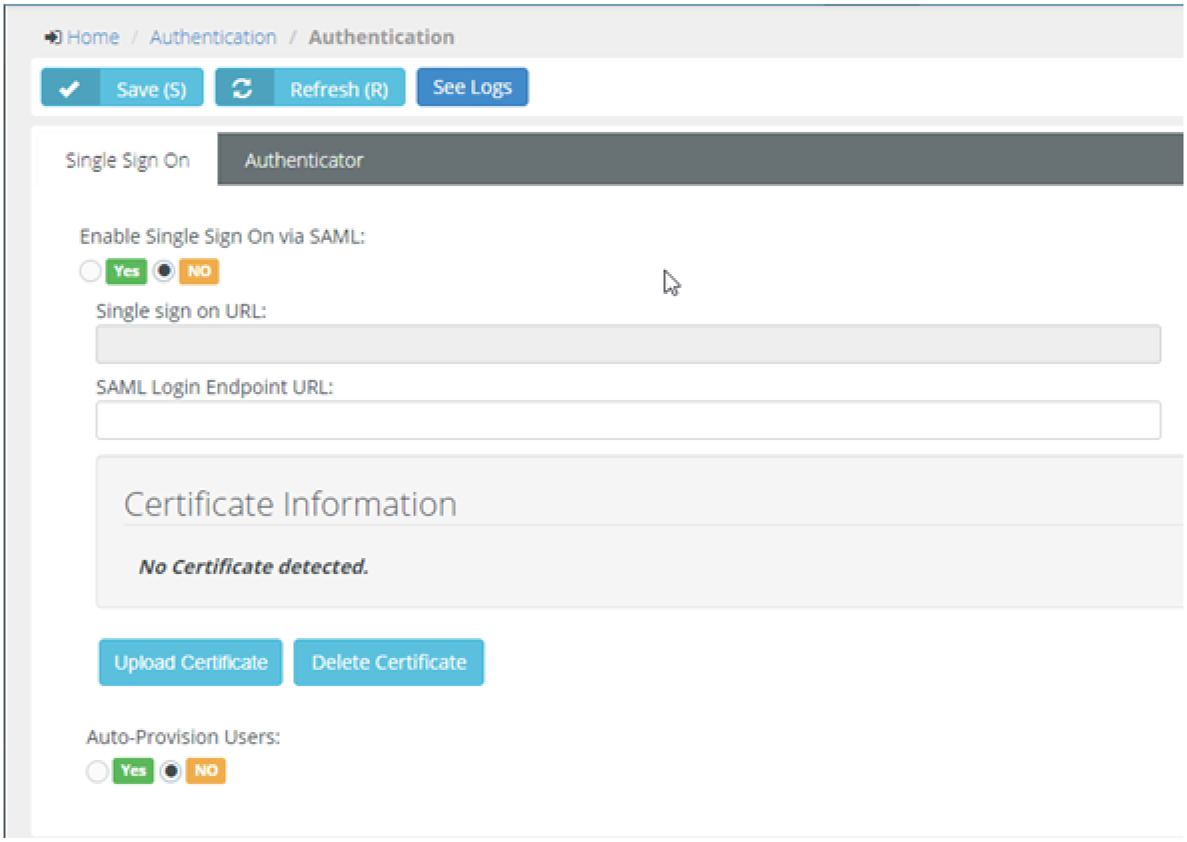
AuthAnvil enables federation by signing and encrypting data sent to the application.

- **Signing Certificate:** Used to sign the token issued to the application with a private key.
  - **Copy Certificate:** Show CER-encoded version of the certificate for easy copying.
  - **Download Certificate:** Download a DER-encoded version of the certificate.
  - **Generate new Certificate:** Generate or upload a new Signing key. **Warning:** You will not be able to sign into the application until it is configured with the new certificate.
- **Encryption Certificate:** Optionally encrypts the token against an application public key.
  - **Copy Certificate:** Show CER-encoded version of the certificate for easy copying.
  - **Download Certificate:** Download a DER-encoded version of the certificate.
  - **Upload new Certificate:** Upload a new encryption key. **Warning:** You will not be able to sign into the application until it is configured with the new certificate.

Vorex Setup

In Vorex we need to setup the system to enable SAML authentication and that can be achieved under **Admin > My Company > Authentication**.

In the “Single Sign On” tab, upload the certificate downloaded previously, and set “Enable Single Sign On via SAML” to **Yes**, then click Save.



Enable Single Sign On via SAML:
○ Yes ● NO

Single sign on URL:

SAML Login Endpoint URL:

Certificate Information

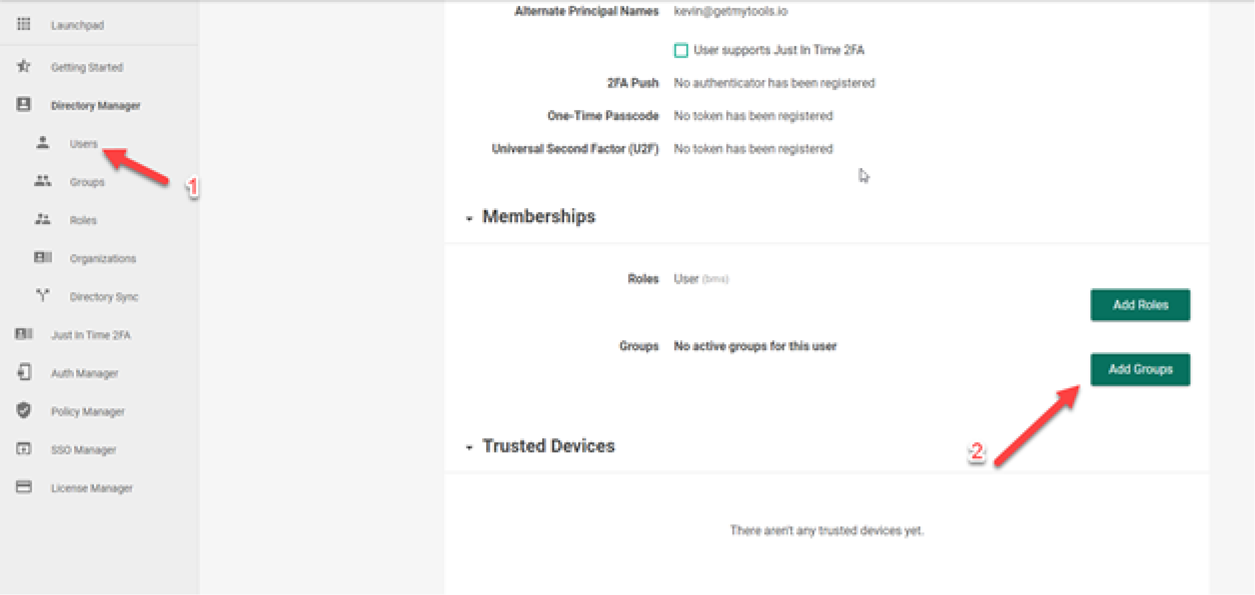
No Certificate detected.

Auto-Provision Users:
○ Yes ● NO

This will enable Vorex SAML authentication.

AuthAnvil Application Assignment

Once the application created, navigate to Directory Manager > Users then choose any user and add the assigned group for this user.



Alternate Principal Names kevin@getmytools.io

□ User supports Just In Time 2FA

2FA Push No authenticator has been registered

One-Time Passcode No token has been registered

Universal Second Factor (U2F) No token has been registered

Memberships

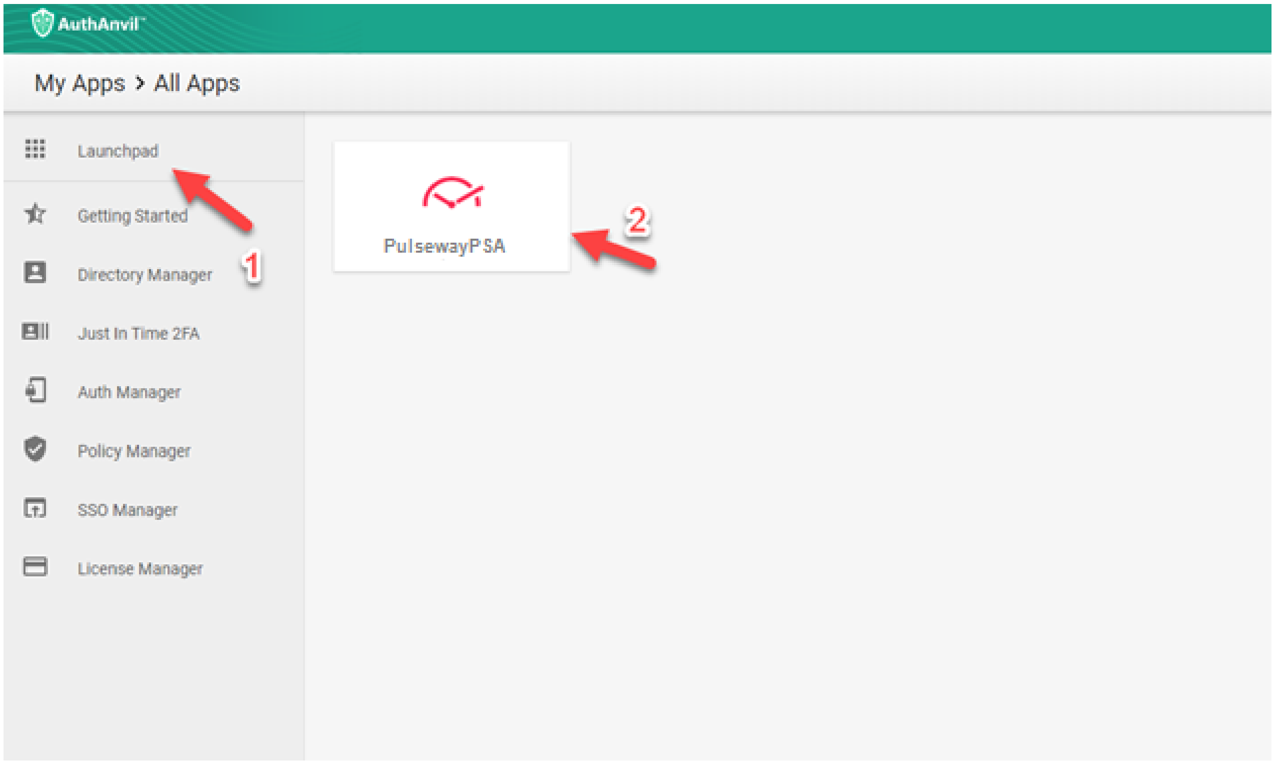
Roles User (bms)

Groups No active groups for this user

Trusted Devices

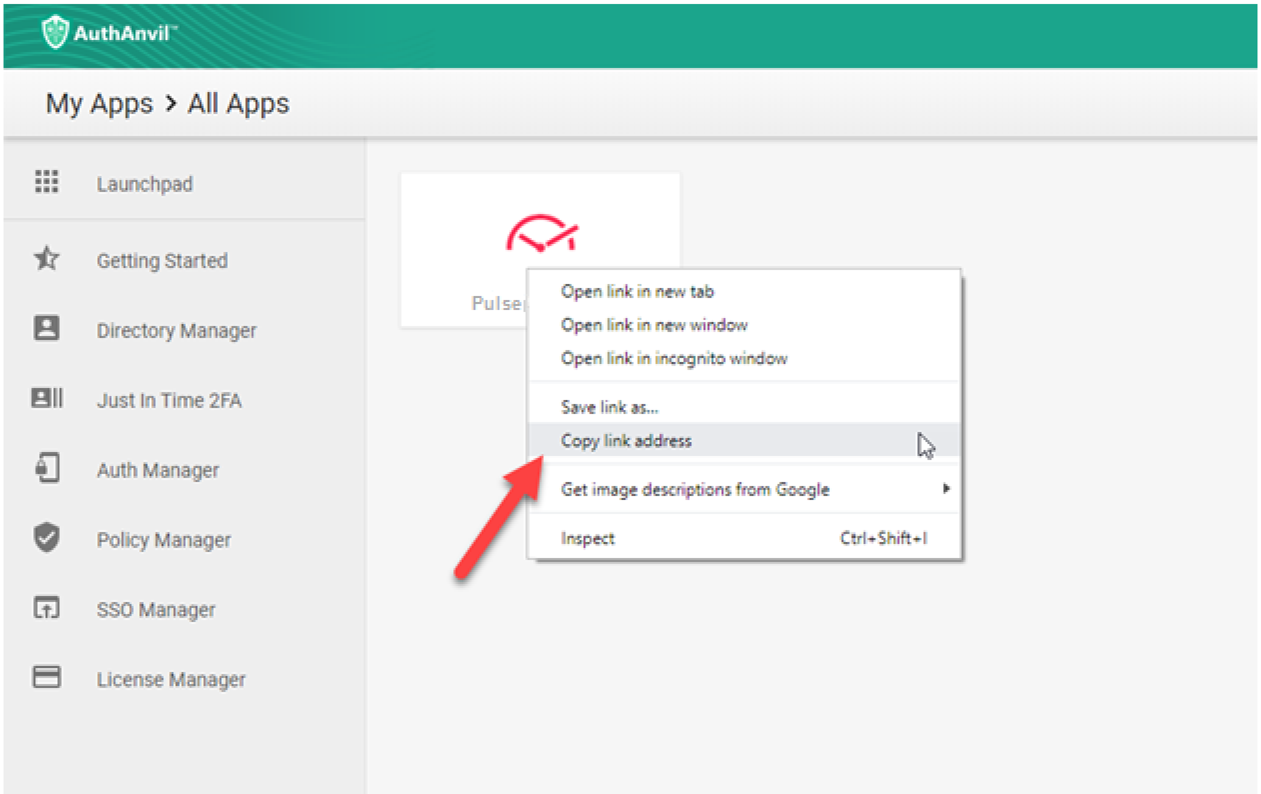
There aren't any trusted devices yet.

Now when the user assigned, go to Launchpad in the left menu then click on the Vorex SSO application you created to be redirected and logged in to Vorex.

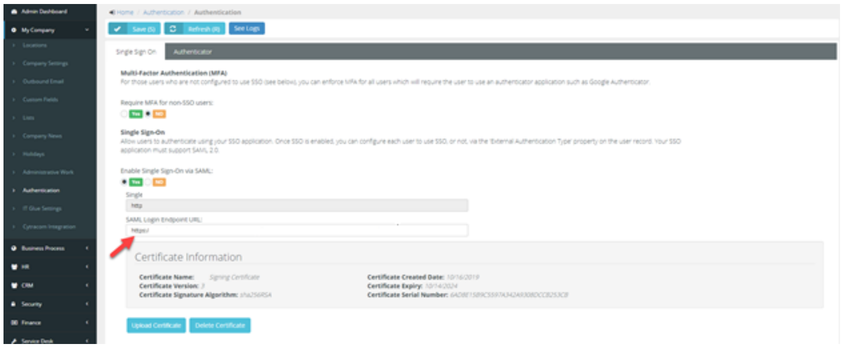

AuthAnvil
My Apps > All Apps
Launchpad
Getting Started
Directory Manager
Just In Time 2FA
Auth Manager
Policy Manager
SSO Manager
License Manager
1
PulsewayPSA
2

Enable Two Way SAML Login

In order to launch AuthAnvil during the Log in from Vorex. You need to enable two-way SAML integration. In order to do this, you will need your AuthAnvil Login URL that can be found here:



Once you have this URL, you will need to save it in Vorex under the Authentication Page:



Multi-Factor Authentication (MFA)
For those users who are not configured to use SSO (see below), you can enforce MFA for all users which will require the user to use an authenticator application such as Google Authenticator.

Require MFA for non-SSO users:
○ Yes ● NO

Single Sign-On
Allow users to authenticate using your SSO application. Once SSO is enabled, you can configure each user to use SSO, or not, via the 'External Authentication Type' property on the user record. Your SSO application must support SAML 2.0.

Enable Single Sign-On via SAML:
● Yes ○ NO

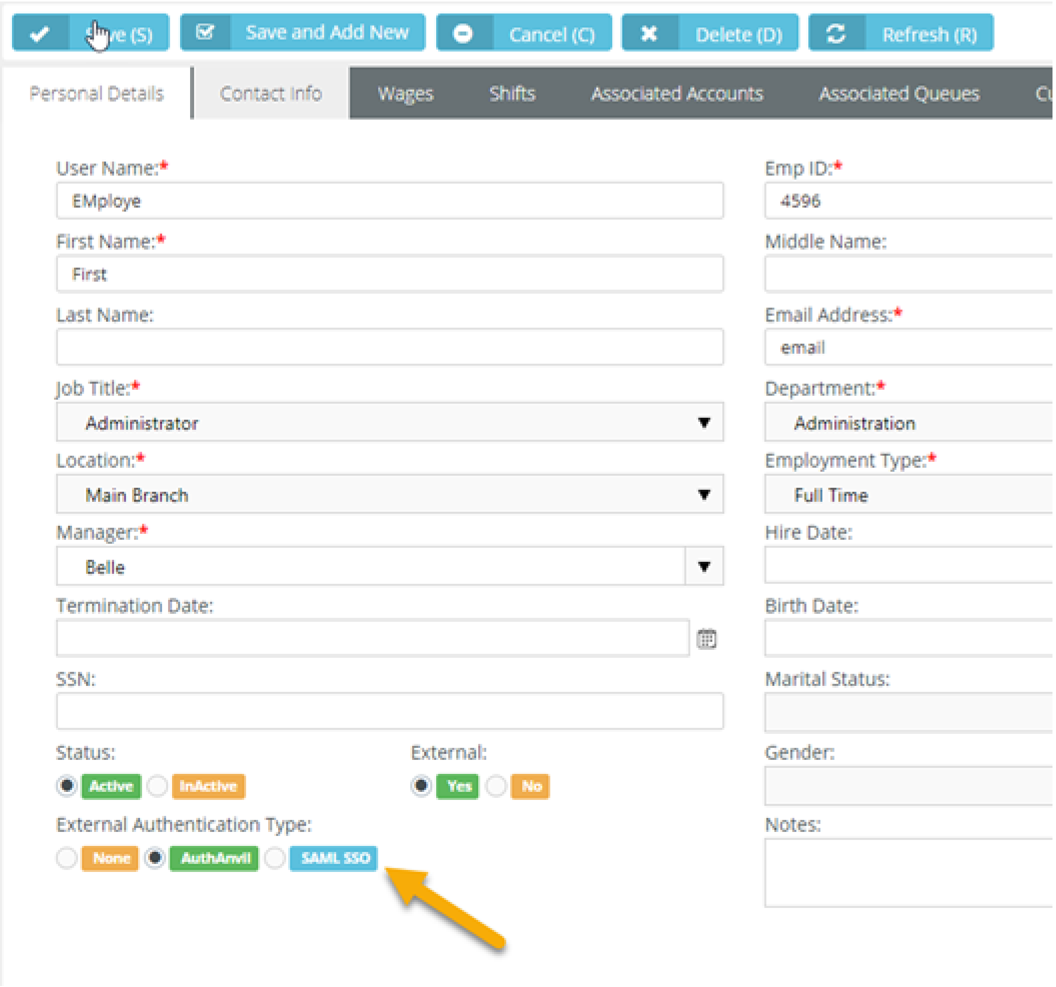
Single
http

SAML Login Endpoint URL:
https:/

Certificate Information

Certificate Name: Signing Certificate
Certificate Version: 3
Certificate Signature Algorithm: sha256RSA
Certificate Created Date: 10/16/2019
Certificate Expiry: 10/14/2024
Certificate Serial Number: 6AD8E1589C5597A342A9308DCCB253CB

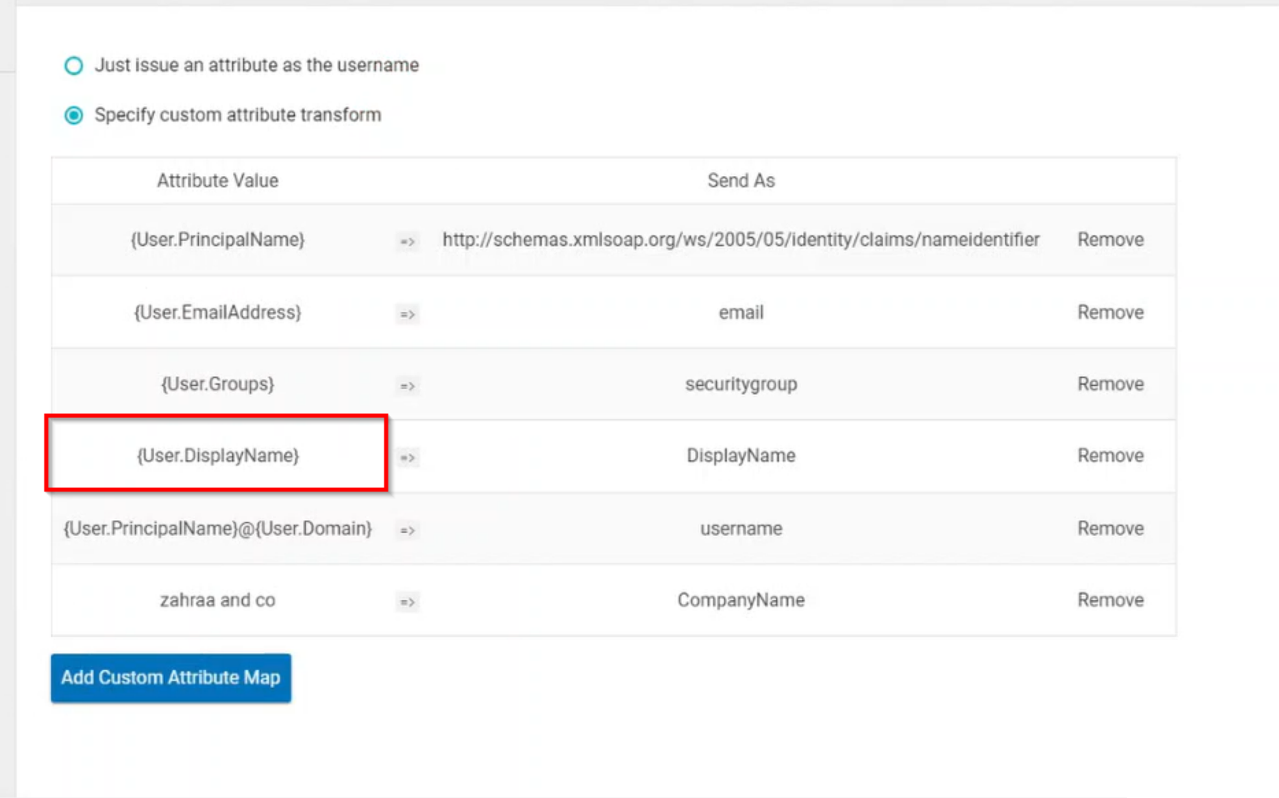
This will allow you to leverage the AuthAnvil Log in screen when users are trying to log in to Vorex. You can enable this on the User Level by updating the Authentication Type on the Employee Level:



User Name:* EMploye	Emp ID:* 4596
First Name:* First	Middle Name:
Last Name:	Email Address:* email
Job Title:* Administrator	Department:* Administration
Location:* Main Branch	Employment Type:* Full Time
Manager:* Belle	Hire Date:
Termination Date:	Birth Date:
SSN:	Marital Status:
Status: ● Active ○ InActive External: ● Yes ○ No	Gender:
External Authentication Type: ○ None ● AuthAnvil ○ SAML SSO	Notes:

Enable JIT Provisioning

IMPORTANT! An additional attribute, `DisplayName` needs to be added in Passly for JIT provisioning.

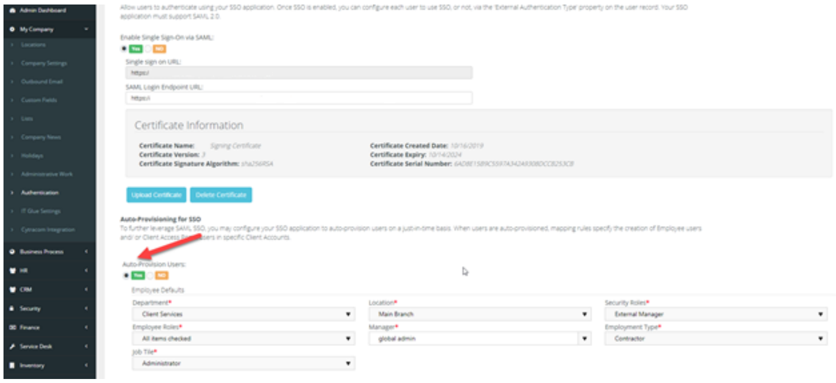


○ Just issue an attribute as the username

● Specify custom attribute transform

Attribute Value		Send As	
{User.PrincipalName}	=>	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	Remove
{User.EmailAddress}	=>	email	Remove
{User.Groups}	=>	securitygroup	Remove
{User.DisplayName}	=>	DisplayName	Remove
{User.PrincipalName}@{User.Domain}	=>	username	Remove
zahraa and co	=>	CompanyName	Remove

In order to enable Just-in-Time (JIT) provisioning, you will need to do it from the Vorex Authentication page.



Allow users to authenticate using your SSO application. Once SSO is enabled, you can configure each user to use SSO, or not, via the 'External Authentication Type' property on the user record. Your SSO application must support SAML 2.0.

Enable Single Sign-On via SAML: ● Yes ○ NO

Single sign on URL: https:/

SAML Login Endpoint URL: https:/i

Certificate Information

Certificate Name: Signing Certificate
Certificate Version: 3
Certificate Signature Algorithm: sha256RSA

Certificate Created Date: 10/16/2019
Certificate Expiry: 10/14/2024
Certificate Serial Number: 6AD8E1589C5597A342493080CC8253C8

Auto-Provisioning for SSO

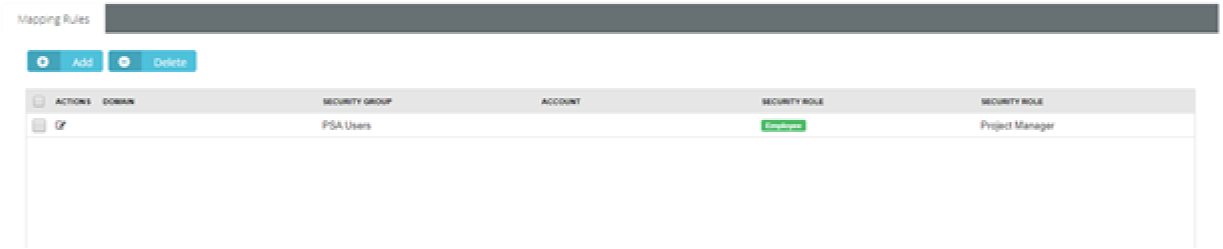
To further leverage SAML SSO, you may configure your SSO application to auto-provision users on a just-in-time basis. When users are auto-provisioned, mapping rules specify the creation of Employee users and/ or Client Access Re[illegible]sers in specific Client Accounts.

Auto-Provision Users: ● Yes ○ NO

Employee Defaults

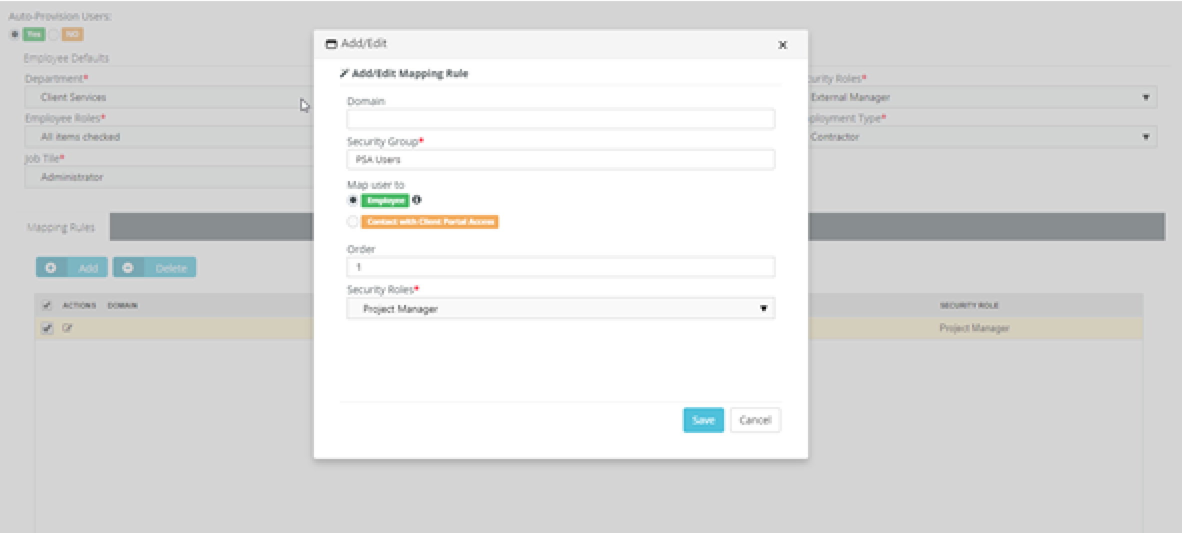
Department*: Client Services
Location*: Main Branch
Security Roles*: External Manager
Employee Roles*: All items checked
Manager*: global admin
Employment Type*: Contractor
Job Title*: Administrator

By default, all Users will take the Default Security Roles specified in the above Employee Defaults Section. In order to start mapping Active Directory Groups to Vorex Security Roles you will need to Add Mapping Rules as following:



□	ACTIONS	DOMAIN	SECURITY GROUP	ACCOUNT	SECURITY ROLE	SECURITY ROLE
□			PSA Users		Employee	Project Manager

By adding multiple Rules, you can now start routing Active Directory Users to Vorex Security Roles based on Domain and Security Group.



Add/Edit Mapping Rule

Domain:

Security Group*: PSA Users

Map user to:
● Employee
○ Contact with Client Portal Access

Order: 1

Security Roles*: Project Manager